FRAGILE BRIDGES. COMPLIANCE MANAGEMENT AMONG CO-OPETING AGENTS

Riccardo Bonazzi, University of Lausanne, Faculty of Economics, Switzerland.
Riccardo.bonazzi@unil.ch

Abstract

This study obtains a set of guidelines with which IS designers can achieve regulatory compliance with data retention requirements. Previous work has explored how to assess compliance threats and to visualize the outcome of policies enforcement but has failed to address how regulatory compliance involves multiple agents seeking to optimize their individual payoffs. We propose a typology that acknowledges in the enterprise business model the return on investment of agents affected by the new controls. Such agents are assumed to be co-opeting, i.e. they gain by cooperating, even if they have different goals. Grounded in control theory and the technology acceptance model, our conceptual design and its implementation represent an economically viable way to align business, legal and IT requirements concerning regulatory compliance with data retention requirements.

Keywords: IT Governance, IT Risk Management, IT Compliance, Design Science, Co-opetition.

1 GENERAL INTRODUCTION

In this study we intend compliance as “the act of adhering to, and the ability to demonstrate adherence to, mandated requirements resulting from contractual obligations and internal policies” (OECG, 2009). Should these policies and standards not be observed, “compliance risk” arises, as described by the Basel Committee on Banking Supervision (2005). Therefore compliance is part of a larger process known as Governance, Risk and Compliance (GRC), which includes the definition of policies (governance) and the mitigation of compliance risk (risk management).

Recent financial scandals have shown the cost for the enterprise of incidents due to a lack of compliance, which can be measured with a metric called Total Cost of Failure (Kahn and Blair, 2004). On the other hand in recent years the Total Cost of Ownership of controls for regulatory compliance can be significantly high. The regulatory risk has even topped the list of business threats perceived by managers (Economist Intelligence Unit, 2005) although some studies (e.g. IT Compliance Policy Group, 2008) report an increase of performance for those who excel in compliance management. Software is there to respond to different compliance needs (McClean, 2009) but it is up to the enterprise to define its requirements, knowing that it does not one single and comprehensive GRC solution.

In the rest of the paper we focus on regulatory requirements concerning information systems for data retention in multinational companies belonging to the financial sector. We believe such problem can be classed as “wicked” (Hevner et al., 2004, p. 81) when an enterprise deals with different businesses in different countries and it has to comply with multiple regulations, which have ambiguous, constantly evolving and sometime conflicting requirements (e.g. the Patriot Act is an American law that requires Swiss banks in U.S. to share data about its customers with American authorities to prevent terrorism; yet the Swiss bank has also to comply with the Swiss regulations concerning customers privacy). Therefore we adopt a design science approach to address such wicked problem.

Accordingly to what said so far our research question is: **How to design information systems for sustainable data retention regulatory compliance among co-opeting agents in heavy regulated business sectors, e.g. multinational financial institutions?**

2 THEORETICAL BACKGROUND

Two main streams of design research have addressed the GRC process: (1) a requirement engineering oriented and (2) a business process oriented. The first stream deals with the first three steps of security management decision process of Straub and Welke (1998) -i.e. risk identification, risk analysis and options analysis - and it tries to achieve compliance by design. Among the large set of papers in this field we refer here only to Giblin et al. (2006), who proposed a solution to pass from enterprise policies to formal requirements, and to Jureta et al. (2010)'s theory of regulatory compliance for requirements engineering. We also acknowledge the existence of IT solutions on the market, as described by Butler and McGovern (2009). Hence once all stakeholders requirements are formalized in order to minimize further adaptations and to achieve compliance by design, cost of controls are claimed to be reduced and this recalls the theoretical claim of the property right approach (Hart and Moore, 1990).

The second stream of research deals with the last two steps of the process. Again, among the many papers that should be cited we refer here to the work of Hoffman et al. (2009) for compliance checking and to Bellamy et al. (2007) for compliance visualization. We also acknowledge the existence of a large set of IT solutions on the market for automatic control and we refer to Rasmussen (2006) for a rough classification. Hence a system is created to automatically collect all user's actions and perform data mining for compliance verification. According to transaction cost theory the gain is claimed to reduce cost of formalization at the requirement level and to increase quality of the process that is controlled.

Once we performed our literature review we have grounded our assessments into practice by performing a four-month full-time internship in the IT compliance team of a major financial institution headquartered in Switzerland. To define controls and rules required, the compliance officer is expected to have a clear understanding of law, business and Information Technology (IT) domains.

From our experience we believe that the existing research has missed to spot three major issues:

(1) The "risk" in business management is a requirement with a return on investment. The decision to comply with a regulation should be seen rather as an option with a cost and expected profits in the future. Therefore we derive the following research sub-question.

RSQ1: How to design sustainable data retention compliance management systems?

(2) We lack a design theory for IT GRC that describes what happens among multiple entities involved, whose intended behavior is neither of conformity nor of deviance. This appears to us as a situation where all actors gain by cooperating, even if they have different goals, as the one described by Nalebuff and Branderburger (1998). Therefore we derive the following research sub-question.

RSQ2: Which are the business model components of a trusted-third party in charge of reducing compliance management cost among co-opeting agents?

(3) Compliance should be represented in the business model as a question of alignment. Since compliance is perceived by many enterprises as a strategic threat, the IT-Law alignment should include the enterprise business model to avoid most compliance risk and reduce the number of required process controls. Therefore we derive the following research sub-question.

RSQ3: How to design sustainable specifications for compliance management among co-opeting agents?

3 RESEARCH METHODOLOGY

According to Hevner et al. (2004:7) design science 'creates and evaluates IT artifacts intended to solve identified organizational problems'. Therefore our process starts with an organizational problem and end with the evaluation of an artifact. Gregor and Jones (2007) go beyond the assumption concerning the advantages of a rigorous process and suggest design research should deliver a theory at the end that extends boundaries beyond the context for which the artifact was developed.

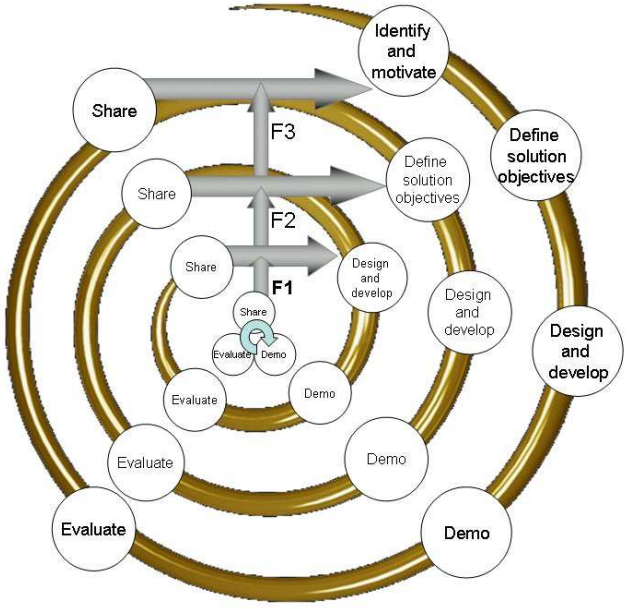

Figure 1. The four loops in our iterative research methodology.

Our starting point is the process proposed by Peffers et al. (2007:54), which has six steps (Identify problem and motivate, Define objective of a solution, Design and Development, Demonstration, Evaluation, Communication). Such process is composed by iterative cycles and has four "entry points", i.e. the researcher can start its research at any step ranging from 1 to 4 depending on the initial conditions. If a design researcher deals with wicked problems, then the four entry points of Peffers et al. (2007) can be seen as maturity level of the same process, which can only go backward if the evaluation stage falsifies previous claims. Such entry points recall the four phases of the approach proposed by Holstrom et al. (2009), which has two exploratory and two explanatory phases. We kept the same name of the tasks that have been used by Peffers et al. (2007). Each iteration occupies a line, associated with a phase of Holstrom et al. (2009). The dashed arrows represent the flows that occur in case the validation phase falsifies the previous results and it refers to the different kind of contribution listed in Locke and Golden-Biddle (1997:1043): addressing incompleteness (F1), inadequacy (F2) or incommensurability (F3). In the following paragraphs we briefly illustrate what has been done in each loop. The results of each loop are going to be presented more in details in the following section.

3.1 Loop 1: Development of an initial solution design

We started by identifying the problem and by motivating the interest of the research community. We wished to address the first gap in the literature and to understand how to design sustainable compliance management systems (RSQ1). The second step in the first loop, i.e. the definitions of the objectives for a solution, also called meta-requirements, was performed with the IT compliance officer. Then we performed action research (Stringer, 1996) to design an artifact to address the problem. In our case the artifact took the shape of a method (the IT GRC workflow) to align business-regulatory and IT requirements. The evaluation of the artifact was descriptive and the results of the first loop were presented to the research community at the workshops of two IS conferences (ICIS and CAISE).

3.2 Loop 2: Refinement of the initial solution design

Once the research community had been acknowledged of the outcomes and feedback had been collected the second loop started. More detailed problem analyses were performed and we extended our scope to economically viable compliance systems among coopeting companies, such as IT outsourcing and open innovation. Hence we performed action research by taking part to a three-month project with a second financial institution. We developed a business model of a third-party in charge of aligning the co-opeting agents. Once again the evaluation of the business model came under the shape of experts opinions from the financial institution. The outcomes have been presented in a workshop of AIS on co-opetition in open innovation and the article has been selected for fast-track by the International Journal of E-Services and Mobile Applications, and it is in its last round before publication.

3.3 Loop 3: Development of substantive theory

Since the results of the second evaluation were consistent with the previous ones, we tried to develop a substantive theory. We initially decided to focus only on data retention for privacy management. This time we worked with a major mobile handsets producer in the telecommunication business, i.e. beyond the financial domain. The theory we aimed to develop in this loop was a mid-range theory under the shape of typology of control actions. We followed the telecommunication firm training course for application programmers and we developed a prototype for privacy management to instantiate a set of control actions for privacy. The description of the prototype has been accepted as a chapter for a book on privacy protection measures and technologies in business organizations. The chosen approach in this loop was action design research (Sein et al. 2011), which is more theory oriented and takes more into account the organizational dimension of the firm. Such approach has been used in two other projects: (1) a multiple case study analysis to derive a typology of IT GRC strategy and (2) a case study within a strategic consultancy to assess the impact of contract design that increases the chance of client and consultant's compliance.

3.4 Loop 4: Development of formal theory

The fourth iteration quantitatively tested the typology of control processes for data retention regulatory compliance, with a special interest in privacy management. Our main goal was to assess the likelihood of success among mobile users of a set of strategies to privacy regulatory compliance. Since our test implied causality we controlled for endogeneity by combining the different control strategies and by obtaining a set of scenario-based surveys. The surveys were given to a large sample (n>150) of mobile users and we assessed the difference in response among respondent groups. Once the different effects of the control actions were assessed we derived a set of business model suggestions for firms in the telecommunication business sector. The formal theory has been briefly presented at the first workshop on mobile business models, whereas the results of the test are about to be published in the special issue on mobile business models of the Journal of Theoretical and Applied Electronic Commerce Research.

4 RESULTS

We start illustrating our results by introducing the concept of ontological distance with the words of Rosemann et al. (2004, p.440): “a label for the extent of the difference between the capabilities embedded within an [Enterprise System] package and the capabilities that an organization needs to be able to operate effectively and efficiently.» In the case of regulatory compliance a company needs to minimize the ontological distance among the three business, IT and regulatory dimensions, which for simplicity we associate here to three agents (one manager per each dimension). We believe that such distance is due to diverging goals among agents, whose behaviors can be described using the Colby and Kohlberg (1987) levels of moral perspective. It can be deviance (to not respect the rules), conformity (to fully agree with the rules) or something in between such as compliance (to respect the rules, even if one does not agree), which is the most likely to occur. Since compliance is a process among coopeting agents, we assume that ontological distance among agents has the tendency to increase over time, unless someone is in charge of aligning the agents’ goals.

4.1 The IT GRC methodology

Our IT GRC methodology is composed of three cycles. The IT governance cycle is in charge of identifying the business opportunity and threats and to steer the firm accordingly to minimize the business risk. The IT risk management cycle is in charge of minimizing the impact of technological (e.g. security) threats over the goals of the company. The compliance management cycle is in charge of assuring that the directives coming from the governance management cycle are understood and executed by risk management cycle, therefore minimizing the regulatory risk. Recalling the alliance management theory of Das and Teng (2001) we claim that agent's perceived ontological distance can be split into agent's perceived regulatory, technological and business risk, which interact among each other. In recent years many IT GRC model appeared but our methodology is still the only one that consider compliance management as between governance and risk management, recognizing its alignment task in addition to control management.

4.2 Business model of a third party for IT GRC

By combining the existing literature in system dynamics, resources-based view, transaction cost and game theories we used the business model ontology of Osterlwader et al. (2005) to obtain the business model components of a third-party agent above. Our claim is that such trusted third-party can align the coopeting agents’ goal into a self-enforcing contract that reduces the agents' perceived ontological distance. Existing research has already proposed different control strategies for infomediaries, and we limited here to cite the most recent work (Koch and Shultze, 2011). But we believe we extend such models by underlying the alignment of third-party value proposition and co-opeting agents’ goals; the required level of trust that the third-party has to acquire by having certifications; the required key

resources that the third-party needs to possess to enable the control strategies to derive an overview of the expected profit and cost of the third party.

4.3 Typology of control actions

Our typology has three main dimensions: regulatory certification, technological solution (process + information technology) and expected return on investment (e.g. profit from avoided legal fee and operational efficiency – cost of technological solution and missed business opportunities). The interactions among the three dimensions can be derived by the theory of Das and Teng (2001) but we are interested here in finding the equilibrium among the three dimensions, since represent an exchange among agents (certification in exchange of technology – technology in exchange of investment – investment in exchange of certification), which has been underlined in the business model of the third party. Therefore we claim that a self-enforcing contract aligns the agents' legal, technological and business goals. The combinations of the three dimensions leads to a set of ideal types, which results in different degree of agent's perceived ontological distance. The purpose of the third-party is to create these ideal types and to assess which of them are really applied in practice. This idea extends the existing goal-oriented requirement engineering approaches, since our approach is mostly decentralized and routed in information economics theory.

5 Testing the typology

The regulatory requirement elicitation and the compliance certification are the bottleneck of the current compliance management cycle. Therefore we tested a solution that allows the ideal types to be extracted by a crowd by a third-party, which can use the crowd also to test the ideal type's likelihood of usage. In our test we fixed the regulatory certification to a privacy regulation in U.K., we checked three different approaches: reduction of collected data, increase of data protection, increase of distributive justice (to exchange the user data with some non-monetary benefit). In our case the co-opeting agents were the mobile user that sends data and the mobile provider that collects the data. As it turns out different groups of mobile users give different scores to these approaches we derived a business model for a third-party in charge of obfuscating the identity of some mobile users and of assuring a proper compensation for the users that are less concerned about privacy. That leads us to claim that self-enforcing contracts goals can be increased by agents' goals elicitated by agents' perceived ontological distance. This extends the works of information systems researchers grounded in psychology, e.g. Cavusoglu et al. (2010), since our intent is to use quantitative results to derive business models prescriptions.

6 CONTRIBUTIONS

Since there is always a tension among practitioners' relevance and theoretical rigor we list a set of suggestions for IT GRC experts, which we derive from our work

Stop hesitating between "control everything" and "trust everyone" strategies. Carefully choose the control level that your firm needs: Our IT methodology shows how agent's perceived ontological distance that leads to coopetition can be split into agent's perceived regulatory, technological and business risk.

Consider the possibility of adding a trusted third-party to decrease compliance management cost: Our third-party business model shows that a self-enforcing contract by a trusted third-party reduces in time the agents' perceived ontological distance

Do not focus only on control: A self-enforcing contract align the agents' legal, technological and business goals

Reduce the cost of compliance management by relying on crowdsourcing to conceive and test the control action ideal types: our test on control ideal types shows that self-enforcing contracts goals can be elicitated by agents' perceived ontological distance.

References

Basel Committee on Banking Supervision, (2005). Compliance and the compliance function in banks, Basel Committee on Banking Supervision.

Bellamy, R. K. E., Erickson, T., Fuller, B., Kellogg, W. A., Rosenbaum, R., Thomas, J. C., & Wolf, T. V. (2007). Seeing is believing: Designing visualizations for managing risk and compliance. IBM Systems Journal, 46(2), 205-218.

Cavusoglu, H., Benbasat, I., & Bulgurcu, B. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly, 34(3), 523-548.

Butler, T., & McGovern, D., (2009). A conceptual model and IS framework for the design and adoption of environmental compliance management systems. Information Systems Frontiers , 1–15.

Colby, A., and Kohlberg, L. (1987). The measurement of moral judgment, Vol. 1: Theoretical foundations and research validation; Vol. 2: Standard issue scoring manual. Cambridge University Press, U.K.. Retrieved on May, the 15th, 2011 from http://books.google.com/

Giblin, C., Muller, S., & Pfitzmann, B., (2006). From regulatory policies to event monitoring rules: Towards model driven compliance automation.

Jones, D., & Gregor, S., (2008). The Anatomy of a Design Theory. Journal of the Association for Information Systems, 8(5), 312-325.

Hart, O., & Moore, J., (1990). Property Rights and the Nature of the Firm. Journal of political economy , 98(6), 1119-1158.

Hevner, A. R., March, S. T., Park, J., & Ram, S., (2004). Design science in information systems research. Management Information Systems Quarterly , 28(1), 75–106.

Holmström, J., Ketokivi, M. & Hameri, A.P., (2009). Bridging Practice and Theory: A Design Science Approach. Decision Sciences , 40(1), 65-87.

Jureta, I., Siena, A., Mylopoulos, J., Perini, A., & Susi, A., (2010). Theory of Regulatory Compliance for Requirements Engineering. Retrieved from http://arxiv.org/pdf/1002.3711

Kahn, R., & Blair, B. T., (2004). Information Nation: Seven Keys to Information Management Compliance. Aiim International.

Koch, H., & Schultze, U. (2011). Stuck in the Conflicted Middle: A Role-Theoretic Perspective on B2B E-Marketplaces. Management Information Systems Quarterly, 35(1), 123-146.

Locke, K. & Golden-Biddle, K., (1997). Constructing opportunities for contribution: Structuring intertextual coherence and" problematizing" in organizational studies. Academy of Management Journal, 1023-1062.

McClean, C., (2009). The GRC Technology Puzzle: Getting All The Pieces To Fit, Report from Forrester Research, Inc.

Nalebuff, B. & Brandenburger, A., (1997). Co-opetition: Competitive and cooperative business strategies for the digital economy. Strategy & Leadership, 25(6), 28-35.

Open Compliance & Ethics Group (OECG) , (2009). Red Book 2.0 (GRC Capability Model). Retrieved from http://www.oceg.org/

Osterwalder, A., Pigneur, Y., & Tucci, C. L., (2005). Clarifying business models: Origins, present, and future of the concept. Communications of the association for Information Systems, 16(1), 1-25.

Peffers, K. et al., (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45-77.

Rasmussen, M., (2006). Overcoming Risk And Compliance Myopia, Report from Forrester Research, Inc.

Roseman, M., Vessey, I. and Weber, R. (2004). Alignment in enterprise systems implementations: The role of ontological distance. In ICIS 2004 Proceedings. Twenty Fifth International Conference on Information Systems ICIS 2004, Washington, DC, (439-447). 9-12 December 2004.

Straub, D. W., & Welke, R. J., (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly , 22(4), 441–469.

Stringer, E. T. (1996). Action Research: A Handbook for Practitioners. 1st edition. Sage Publications, Inc. U.S.A.